Research Statement

Qin Wang[1,2]

[1] *Swinburne University of Technology, Melbourne, Australia*
[2] *CSIRO Data61, Sydney, Australia*
qinwang@swin.edu.au

I'm broadly interested in blockchain and cryptocurrencies. My research focuses on the core components (structure, consensus, smart contract, etc.) and fundamental properties (security, scalability, applicability, etc.) of blockchain systems. My work mainly combines the techniques from applied cryptography and distributed computing systems. Currently, I'm working on topics as listed.

Blockchain scalability. Performance bottlenecks (slow confirmation and poor scalability) of blockchain systems retard their adoptions and applications. One of the main reasons comes from their linear-structured designs (such as in Bitcoin, Ethereum). Linear-sequenced blocks result in severe consumption of resources because only one block in each round will be deemed as valid/confirmed among many competitive blocks. To solve such issues, we explore the Directed Acyclic Graph (DAG)-based techniques. These systems, instead, structure transactions/blocks in the form of graphs. This indicates multiple blocks can be accepted at the same time. The promise of DAG-based blockchain systems is to enable fast confirmation (complete transactions within million seconds) and high scalability (attach transactions in parallel) without significantly compromising security. My research in this line includes the overview of existing systems [WYCX20], the simulation of typical projects [WCYW20] [WWCX20], and innovative improvements [WL21].

Blockchcain security analysis. Blockchain security includes many aspects that can be classified by its components. My work focuses on its core component – consensus mechanisms/protocols. Consensus provides a powerful means of establishing agreement as to the network's current state, and it is critical for maintaining the consistency of states and long-lasting operation of entire systems. Many *in-the-wild* projects propose their customized consensus protocols, but most of them have not been strictly proved. My research in this line contains the security analysis on variety types of protocols, covering BFT-style protocols [W$^+$20][WLCX21], DAG-based consensus [WWCX20], and PoX-style protocols like proof-of-authority (PoA).

Privacy-preserving techniques. Blockchain provides a completely transparent environment for deploying distributed applications. The states of the protocols are publicly accessible by any participant that may include malicious users. An adversary may keep tracing an account with a huge amount of coins, and obtain its linkage towards real identities through offline activities. Simple pseudonym provided in traditional ways (e.g., addresses) is insufficient. The absence of privacy protection of user identification and sensitive information limits the usage of an entire range of applications that rely on privacy. My research in this line proposes multiple ways of enhancing privacy, both on transaction and (smart contract) states. The main approach is to leverage crypto-techniques such as homomorphic encryption (HE) [WQHX17][WCX21] certificate encryption (CBE) [WLWG], public key infrastructure (PKI) [QHW+20], and hardware-assisted environments (e.g. TEE) [LWZ+21][LWL+20]. Further, my work also explores the applications of confidential blockchain in real scenarios like electricity bills [WH+20].

Blockchain economics (DeFi/NFT/FinTech). Blockchain shapes finance by removing intermediaries that provide financial instruments (e.g. exchanges, central banks, and brokerages). By smart contracts, the blockchain-based form of finance obtains plenty of advanced properties such as decentralization, automation, tractability, transparency, and non-repudiation. Also, it stimulates a lot of prevailing concepts like FinTech, DeFi, ICO, NFT, etc. However, many challenges still exist when facing real-world financial scenarios that require liquidity, interoperability, and high-level security. Currently, my research of this line [WLWC21] explores state-of-the-art NFT solutions, an emerging market used to trade/auction/exchange digital properties and collectible like stamps, art, music, video, or even virtual animals.

References

[LWL+20] Rujia Li, Qin Wang, Feng Liu, Qi Wang, and David Galindo. An accountable decryption system based on privacy-preserving smart contracts. In *International Conference on Information Security*, pages 372–390. Springer, 2020.

[LWZ+21] Rujia Li, Qin Wang, Xinrui Zhang, Qi Wang, David Galindo, and Yang Xiang. An offline delegatable cryptocurrency system. *arXiv preprint arXiv:2103.12905*, 2021.

[QHW+20] Bo Qin, Jikun Huang, Qin Wang, Xizhao Luo, Bin Liang, and Wenchang Shi. Cecoin: A decentralized pki mitigating mitm attacks. *Future Generation Computer Systems*, 107:805–815, 2020.

[W+20] Qin Wang et al. Security analysis on dbft protocol of neo. In *International Conference on Financial Cryptography and Data Security (FC)*, pages 20–31. Springer, 2020.

[WCX21] Qin Wang, Shiping Chen, and Yang Xiang. Anonymous blockchain-based system for consortium. *ACM Transactions on Management Information Systems (TMIS)*, 12(3):1–25, 2021.

[WCYW20] Bozhi Wang, Shiping Chen, Lina Yao, and Qin Wang. Chainsim: A p2p blockchain simulation framework. In *CCF China Blockchain Conference*, pages 1–16. Springer, 2020.

[WH+20] Qin Wang, Longxia Huang, et al. Blockchain enables your bill safer. *IEEE Internet of Things Journal*, 2020.

[WL21] Qin Wang and Rujia Li. A weak consensus algorithm and its application to high-performance blockchain. *arXiv preprint arXiv:2102.00872*, 2021.

[WLCX21] Qin Wang, Rujia Li, Shiping Chen, and Yang Xiang. Formal security analysis on dbft protocol of neo. *arXiv preprint arXiv:2105.07459*, 2021.

[WLWC21] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*, 2021.

[WLWG] Qin Wang, Rujia Li, Qi Wang, and David Galindo. Poster: Transparent certificate revocation for cbe based on blockchain.

[WQHX17] Qin Wang, Bo Qin, Jiankun Hu, and Fu Xiao. Preserving transaction privacy in bitcoin. *Future Generation Computer Systems*, 2017.

[WWCX20] Bozhi Wang, Qin Wang, Shiping Chen, and Yang Xiang. Security analysis on tangle-based blockchain through simulation. In *Australasian Conference on Information Security and Privacy*, pages 653–663. Springer, 2020.

[WYCX20] Qin Wang, Jiangshan Yu, Shiping Chen, and Yang Xiang. Sok: Diving into dag-based blockchain systems. *arXiv preprint arXiv:2012.06128*, 2020.